**用户指南**

**1.基础二进制加解密**  
此功能用于对单组8位的二进制数据进行加密或解密。

1.切换到基础加解密标签页。

2.在“8位输入(二进制)”框中，输入你的8位明文或密文（例如10101010）。

3.在“10位密钥(二进制)”框中，输入用于计算的10位密钥（例如1100110011）。

4.点击“加密”或“解密”按钮。

5.结果将立刻显示在“输出结果”框中。  


**2.ASCII 字符串加解密**

此功能用于对一段文本字符串进行加密或解密。

1.切换到字符串处理标签页。

2.在“输入文本”框中，输入你想要处理的字符串（例如Hello）。

3.在“10位密钥(二进制)”框中，输入10位密钥。

4.点击“加密字符串”或“解密字符串”按钮。

5.处理后的结果会显示在下方的“输出结果”框中。

（加密后的文本通常会显示为无意义的乱码，这是正常现象。）  


**3.密钥暴力破解**  
当你拥有明文和对应的密文时，此功能可以自动找出加密所使用的密钥。

1.切换到暴力破解标签页。

2.首先在“破解模式”下拉菜单中选择binary（二进制）或ascii（字符串）。

3.根据所选模式，在“已知明文”和“对应密文”框中输入你的数据。

4.点击“开始暴力破解”按钮。

5.程序将开始遍历所有1024个密钥，进度条会显示当前进度。

6.破解完成后，所有找到的可能密钥、耗时等信息将显示在“破解结果”区域。  
  
**4.算法特性分析**  
此功能用于分析S-DES算法是否存在“密钥碰撞”，即多个不同的密钥将同一个明文加密成同一个密文的现象。

1.切换到算法分析标签页。

2.在“8位明文(二进制)”框中，输入一个你希望进行分析的8位二进制明文。

3.点击“开始算法分析”按钮。

4.程序将使用所有密钥对该明文进行加密，并通过进度条展示进度。

5.分析完成后，结果将显示在“分析结果”区域。如果存在密钥碰撞，这里会详细列出是哪个密文以及由哪些不同的密钥生成。  
